PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	09/992,310
Filing Date:	November 19, 2001
Applicant:	Laurence I. Rockwell
Group Art Unit:	2617
Examiner:	Randy Peaches
Title:	AIRBORNE SECURITY MANAGER
Attorney Docket:	7784-000188

Mail Stop Appeal Brief-Patents
Director of The United States Patent and Trademark Office
Trademark Trial and Appeal Board
P.O. Box 1451
Alexandria, Virginia 22313-1451

AMENDED APPEAL BRIEF UNDER 37 C.F.R § 41.37(a)

Sir:

This is an amended appeal brief in support of an appeal to the U.S. Patent and Trademark Office Board of Patent Appeals and Interferences (the "Board") from the September 28, 2006 Notice of Panel Decision from Pre-Appeal Brief Review rejecting Claims 20-39 and the prior Final Rejection mailed February 22, 2006 rejecting Claims 20-28, 30, 31 and 34, however, only Claims 20-28, 30, 31 and 34-39 were pending. This appeal brief is being filed in accordance with 37 C.F.R. § 41.37, within one month from mailing of the Notice of Panel Decision

from Pre-Appeal Brief Review mailed September 28, 2006 from the U.S. Patent and Trademark Office.

REAL PARTY IN INTEREST

The Boeing Company, being the assignee of the present application, is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences pending which will directly affect or be directly affected by, or have a bearing on, the Board's decision in the present pending appeal. It should be noted that on May 22, 2006 Appellant Requested a Pre-Appeal review.

STATUS OF CLAIMS

On October 4, 2006, Appellant received the Panel Decision of the Pre-Appeal Review Board affirming the rejection of Claims 20-39, however, only Claims 20-28, 30, 31 and 34-39 are finally rejected. In this regard, Claims 2 and 13 were cancelled in Appellant's Amendment filed October 20, 2004, Claims 1, 3-12 and 14-19 were cancelled in Appellant's Amendment filed on July 8, 2005 and Claims 29, 32 and 33 were cancelled in Appellant's Amendment filed on November 28, 2005. Accordingly, Claims 20-28, 30, 31 and 34-39 remain finally rejected.

STATUS OF AMENDMENTS

No amendments have been filed subsequent to the final Office Action of February 22, 2006.

SUMMARY OF CLAIMED SUBJECT MATTER

The following summarizes Appellant's subject matter as presented in independent Claims 20, 28, 34 and 38:

Initially, as an overview, all of the independent claims relate to an airborne security management system for monitoring security activities in a mobile network platform, and more particularly to an autonomous airborne security manager for responding to detected security intrusion events when the mobile network platform is or is not in communication with a terrestrial-based network security management system (Paragraph [0002]; p. 1, lines 9-13, (Figure 1)).

RECITATION OF SPECIFIC FEATURES PRESENTED IN THE INDEPENDENT CLAIMS

Independent Claim 20

Figure 1 illustrates a network security architecture 10 for monitoring security activities in an unattended mobile network platform 12. The primary purpose of the network security architecture 10 is to monitor, record, report and respond to security-relevant events associated with the mobile network platform 12. The network security architecture 10 supports a mobile network platform residing in an aircraft. The mobile network platform 12 is in turn interconnected via one or more unreliable wireless communication links 14 to a terrestrial-based

communication system 16, including a terrestrial-based network security management system 18. (Paragraph [0016]; p. 5, lines 7-14, (Figure 1)). The cabin distribution subsystem (CDS) 28 provides network connectivity through a plurality of user access points to the passengers of the aircraft. (Paragraph [0023], p. 8, lines 7-8 (Figure 1)).

The airborne security manager 34 is responsible for enforcing security policy for an aircraft. Because communication with the aircraft may be sporadic, the airborne security manager 34 must provide the capability to act autonomously when responding to security intrusion events. When a security intrusion event is detected, the airborne security manager 34 responds appropriately in accordance with a customizable security policy. Thus, the airborne security manager 34 is adapted to receive security intrusion events from any of the intrusion detection subsystems and operable to implement a security response. (Paragraph [0022]; p. 7, lines 17-20, p. 8, lines 1-4 (Figure 1)).

With reference to Figure 5, the airborne security manager 34 is further comprised of five functional modules: an event response module 72, an onboard status module 74, a policy manager 76, a persistent storage manager 78, and a communication manager 80. The event response module 72 is responsible for receiving events, interpreting the active security policy, and triggering the appropriate actions in response to each event. It should be appreciated that this module is adapted to handle events other than security intrusion events received from the intrusion detection subsystems. (Paragraph [0031]; p. 13, lines 13-19, (Figure 5)).

In conjunction with the onboard status module 74, the event response module interprets and executes the state machine representing the active security policy. For instance, upon arrival of a security intrusion event, the event response module determines whether the event is associated with an individual passenger connection, an individual host server, or the airborne security manager as a whole. This module then retrieves the current state of that passenger connection, host server, or airborne security manager from the onboard status module 74 and performs the actions associated with that state and event in accordance with the active security policy. Exemplary actions may include issuing new events, making state transitions, modifying network filters, disabling passenger connections, and/or queuing messages for transmission to the terrestrial-based network security management system. (Paragraph [0034]; p. 13, line 20, p. 14 lines 1-10, (Figure 5)).

If an update to the security policy is necessary, the policies are updated during the time that the intermittent link has a connection (Paragraph [0045], p. 18 lines 13-18, (Figure 5); Paragraph [0046], p. 18 lines 19-20, p. 19 lines 1-3, (Figure 5); Paragraph [0049], p. 20 lines 17-20, p. 21 lines 1-9, (Figure 8); Paragraph [0050], p. 21 lines 10-19, (Figures 1, 8).

Independent Claim 28

Figure 1 illustrates a network security architecture 10 for monitoring security activities in an unattended mobile network platform 12. The primary purpose of the network security architecture 10 is to monitor, record, report and respond to security-relevant events associated with the mobile network platform

12. The network security architecture 10 supports a mobile network platform residing in an aircraft. The mobile network platform 12 is in turn interconnected via one or more unreliable wireless communication links 14 to a terrestrial-based communication system 16, including a terrestrial-based network security management system 18. (Paragraph [0016]; p. 5, lines 7-14, (Figure 1)).

The airborne security manager 34 is responsible for enforcing security policy for an aircraft. Because communication with the aircraft may be sporadic, the airborne security manager 34 must provide the capability to act autonomously when responding to security intrusion events. When a security intrusion event is detected, the airborne security manager 34 responds appropriately in accordance with a customizable security policy. Thus, the airborne security manager 34 is adapted to receive security intrusion events from any of the intrusion detection subsystems and operable to implement a security response. Exemplary responses may include warnings one or more passengers on the aircraft, alerting terrestrial-based security administrators, and/or disconnecting a passenger's network access. (Paragraph [0022] p. 7, lines 17-20, p. 8, lines 1-4 (Figure 1)).

The cabin distribution subsystem (CDS) 28 provides network connectivity through a plurality of user access points to the passengers of the aircraft. (Paragraph [0023], p. 8, lines 7-8 (Figure 1)). In Figure 2A, each user access point can be in one of three defined states. By default, all user access points begin in a normal state 42. A security intrusion event of any kind will result in a transition to either a suspected state 44 or a disconnected state 46 for the

applicable user access point. Each transition is in the form of "event/response" where events are the external triggers that cause the state transition and responses are external actions that the system initiates when making the transition. For instance, a low or medium priority event 48 occurring in a normal state will cause the system to log the event and/or attempt to provide a warning to the passenger connected at that user access point. The user access point then transitions to the suspected state as shown in Figure 2A. (Paragraph [0027], p. 27 lines 11-20 (Figures 1, 2A)).

With reference to Figure 5, the airborne security manager 34 is further comprised of five functional modules: an event response module 72, an onboard status module 74, a policy manager 76, a persistent storage manager 78, and a communication manager 80. The event response module 72 is responsible for receiving events, interpreting the active security policy, and triggering the appropriate actions in response to each event. It should be appreciated that this module is adapted to handle events other than security intrusion events received from the intrusion detection subsystems. (Paragraph [0031]; p. 13, lines 13-19, (Figure 5)).

In conjunction with the onboard status module 74, the event response module interprets and executes the state machine representing the active security policy. For instance, upon arrival of a security intrusion event, the event response module determines whether the event is associated with an individual passenger connection, an individual host server, or the airborne security manager as a whole. This module then retrieves the current state of that

passenger connection, host server, or airborne security manager from the onboard status module 74 and performs the actions associated with that state and event in accordance with the active security policy. Exemplary actions may include issuing new events, making state transitions, modifying network filters, disabling passenger connections, and/or queuing messages for transmission to the terrestrial-based network security management system. (Paragraph [0034]; p. 13, line 20, p. 14 lines 1-10, (Figure 5)).

If an update to the security policy is necessary, the policies are updated during the time that the intermittent link has a connection (Paragraph [0045], p. 18 lines 13-18, (Figure 5); Paragraph [0046], p. 18 lines 19-20, p. 19 lines 1-3, (Figure 5); Paragraph [0049], p. 20 lines 17-20, p. 21 lines 1-9, (Figure 8); Paragraph [0050], p. 21 lines 10-19, (Figures 1, 8).

Independent Claim 34

Figure 1 illustrates a network security architecture 10 for monitoring security activities in an unattended mobile network platform 12. The primary purpose of the network security architecture 10 is to monitor, record, report and respond to security-relevant events associated with the mobile network platform 12. The network security architecture 10 supports a mobile network platform residing in an aircraft. The mobile network platform 12 is in turn interconnected via one or more unreliable wireless communication links 14 to a terrestrial-based communication system 16, including a terrestrial-based network security management system 18. (Paragraph [0016]; p. 5, lines 7-14, (Figure 1)).

The airborne security manager 34 is responsible for enforcing security policy for an aircraft. Because communication with the aircraft may be sporadic, the airborne security manager 34 must provide the capability to act autonomously when responding to security intrusion events. When a security intrusion event is detected, the airborne security manager 34 responds appropriately in accordance with a customizable security policy. Thus, the airborne security manager 34 is adapted to receive security intrusion events from any of the intrusion detection subsystems and operable to implement a security response. Exemplary responses may include warnings one or more passengers on the aircraft, alerting terrestrial-based security administrators, and/or disconnecting a passenger's network access. (Paragraph [0022] p. 7, lines 17-20, p. 8, lines 1-4 (Figure 1)).

The cabin distribution subsystem (CDS) 28 provides network connectivity through a plurality of user access points to the passengers of the aircraft. (Paragraph [0023], p. 8, lines 7-8 (Figure 1)). In Figure 2A, each user access point can be in one of three defined states. By default, all user access points begin in a normal state 42. A security intrusion event of any kind will result in a transition to either a suspected state 44 or a disconnected state 46 for the applicable user access point. Each transition is in the form of "event/response" where events are the external triggers that cause the state transition and responses are external actions that the system initiates when making the transition. For instance, a low or medium priority event 48 occurring in a normal state will cause the system to log the event and/or attempt to provide a warning

to the passenger connected at that user access point. The user access point then transitions to the suspected state as shown in Figure 2A. (Paragraph [0027], p. 27 lines 11-20 (Figures 1, 2A)).

With reference to Figure 5, the airborne security manager 34 is further comprised of five functional modules: an event response module 72, an onboard status module 74, a policy manager 76, a persistent storage manager 78, and a communication manager 80. The event response module 72 is responsible for receiving events, interpreting the active security policy, and triggering the appropriate actions in response to each event. It should be appreciated that this module is adapted to handle events other than security intrusion events received from the intrusion detection subsystems. (Paragraph [0031]; p. 13, lines 13-19, (Figure 5)).

Independent Claim 38

Figure 1 illustrates a network security architecture 10 for monitoring security activities in an unattended mobile network platform 12. The primary purpose of the network security architecture 10 is to monitor, record, report and respond to security-relevant events associated with the mobile network platform 12. The network security architecture 10 supports a mobile network platform residing in an aircraft. The mobile network platform 12 is in turn interconnected via one or more unreliable wireless communication links 14 to a terrestrial-based communication system 16, including a terrestrial-based network security management system 18. (Paragraph [0016]; p. 5, lines 7-14, (Figure 1)).

The airborne security manager 34 is responsible for enforcing security policy for an aircraft. Because communication with the aircraft may be sporadic, the airborne security manager 34 must provide the capability to act autonomously when responding to security intrusion events. When a security intrusion event is detected, the airborne security manager 34 responds appropriately in accordance with a customizable security policy. Thus, the airborne security manager 34 is adapted to receive security intrusion events from any of the intrusion detection subsystems and operable to implement a security response. Exemplary responses may include warnings one or more passengers on the aircraft, alerting terrestrial-based security administrators, and/or disconnecting a passenger's network access. (Paragraph [0022] p. 7, lines 17-20, p. 8, lines 1-4 (Figure 1)).

The cabin distribution subsystem (CDS) 28 provides network connectivity through a plurality of user access points to the passengers of the aircraft. (Paragraph [0023], p. 8, lines 7-8 (Figure 1)). In Figure 2A, each user access point can be in one of three defined states. By default, all user access points begin in a normal state 42. A security intrusion event of any kind will result in a transition to either a suspected state 44 or a disconnected state 46 for the applicable user access point. Each transition is in the form of "event/response" where events are the external triggers that cause the state transition and responses are external actions that the system initiates when making the transition. For instance, a low or medium priority event 48 occurring in a normal state will cause the system to log the event and/or attempt to provide a warning

to the passenger connected at that user access point. The user access point then transitions to the suspected state as shown in Figure 2A. (Paragraph [0027], p. 27 lines 11-20 (Figures 1, 2A)).

With reference to Figure 5, the airborne security manager 34 is further comprised of five functional modules: an event response module 72, an onboard status module 74, a policy manager 76, a persistent storage manager 78, and a communication manager 80. The event response module 72 is responsible for receiving events, interpreting the active security policy, and triggering the appropriate actions in response to each event. It should be appreciated that this module is adapted to handle events other than security intrusion events received from the intrusion detection subsystems. (Paragraph [0031]; p. 13, lines 13-19, (Figure 5)).

GROUNDS FOR REJECTION TO BE REVIEWED ON APPEAL

Appellant presents the following issue for review:

Whether Claims 20-28, 30-31 and 34-49 are anticipated under 35 U.S.C. 103(a) by Huff et al. (U.S. Pat. No. 6,408,391, hereinafter "Huff") in view of Monroe (U.S. Pat. No. 6,392,692, hereinafter "Monroe").

ARGUMENTS

I. THE EXAMINER'S RATIONALE

The Examiner provided one rationale in rejecting claims 20-28, 30-31 and 34-39 as stated in his final rejection mailed February 22, 2006. The Examiner states it would have been obvious to one of skill in the art to modify the security

system of Huff with the terrestrial-based system of Monroe to arrive at the claimed security system for a mobile platform.

II. INTRODUCTION

Huff appears to disclose only a system for monitoring either authorized or unauthorized users by two security servers 500, 600 that are located on trucks 700, 732 (see at least Column 13, Lines 47-67 and Column 14, Lines 4-11). Each of the security servers 500, 600, communicate with three other peer-to-peer links, 720, 730 and 740 each at different frequencies. Each of the peer-to-peer links 720, 730 and 740 in Huff includes one computer disposed on each vehicle (722, 24, 726; 734, 736; 742, 744 respectively), while the security servers 500, 600 are each disposed on a wholly separate vehicle (trucks 700, 732) to monitor each computer disposed on each vehicle in the peer-to-peer links, 720, 730, 740 (see at least Column 14, lines 19-28). One of the vehicles in the peer-to-peer links, 720, 730 and 740, serves as a hub to enable communication between the remaining vehicles and the server 500.

Monroe appears to disclose an electronic surveillance system which "provides both visual and/or audio information as well as critical data such as location, direction, intrusion, fire and/or smoke detection...." The primary purpose of Monroe is monitoring the mobile platform "while in port or terminal and/or unattended whether taxing or parked or docked [and] permits tracking while in port or in route [to the port]" through a ground-based communications link (see at least Column 2, Lines 30-51). Monroe further discloses notifying "selected

personnel" of a security situation on the mobile platform (see at least Column 7, Lines 59-60).

In contrast to Huff and Monroe, Appellant's disclosure provides an onboard network accessible to a plurality of users or an intrusion detection system onboard a mobile platform and connected to the onboard network. Appellant also notes that the system and method of the present application does not suffer from the potential drawbacks of Huff because, with the present system, the server(s) are on the same mobile platform as all the network access points that are being monitored. With Huff, since the important servers are on separate mobile platforms from the access points they are monitoring, a loss of communication link with any of the individual trucks can destroy the effectiveness of the whole monitoring system. With the present system, since the server(s) are on the same mobile platform with the access points they are monitoring, the present system is not susceptible to this potential "breakdown" in security from which the Huff system would appear to suffer.

III. THE EXAMINER HAS FAILED TO ESTABLISH A *PRIMA FACIE* CASE OF OBVIOUSNESS

It is well settled that "a *prima facie* case of obviousness is established when the teachings from the prior art itself would appear to have suggested the claimed subject matter to a person of ordinary skill in the art." *In re Rinehart*, 531 F2d 1048, 1049 (U.S. Ct. of Customs and Patent Appeals, 1976). The U.S. Supreme Court has identified three primary criteria for establishing obviousness. These are: 1) determination of the scope and content of the prior art; 2)

determination of the differences between the prior art and the claims at issue; and 3) determination of the level of ordinary skill in the pertinent art. *Graham v. John Deere*, 383 U.S. 1, 17 (1966). In rejecting claims under 35 U.S.C. §103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. See *In re Fine*, 837 F.2d 1071, 1073, (Fed. Cir. 1988). In so doing, the Examiner is expected to make the factual determinations set forth as noted above in *Graham v. John Deere,* and to provide a reason why one having ordinary skill in the pertinent art would have been led to modify the prior art or to combine prior art references to arrive at the claimed invention.

In the case *In re Vaeck*, the Federal Circuit noted that two criteria must be met for *prima facie* obviousness to exist: 1) there must be some suggestion or motivation in the references or generally available knowledge to a person of skill in the arts to modify or combine the references; and 2) there must be a reasonable expectation of success. Both the motivation and the reasonable expectation of success must be found in the prior art and not in the Appellant's disclosure. 947 F2d 488, 493 (Fed. Cir. 1991). See also *Uniroyal, Inc. v. Rudkin-Wiley Corp.*, 837 F.2d 1044, 1051 (Fed. Cir.) cert. denied, 488 U.S. 825 (1985). These showings by the Examiner are an essential part of complying with the burden of presenting a *prima facie* case of obviousness. Note, *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992). Appellant respectfully asserts that none of the references cited by the Examiner teach or suggest an onboard network accessible to a plurality of users or an intrusion detection system onboard a mobile platform connected to the onboard network, as claimed. In addition, it is

improper to combine Huff with Monroe to arrive at Appellant's claimed subject matter, as Huff teaches away from this modification. In particular, independent Claim 20 recites:

> an intrusion detection system **onboard** the mobile platform and connected to the onboard network; and . . .
>
> **wherein, if an update is necessary, the policies being updated during the time that the intermittent link has connection (emphasis added).**

Claim 28 recites:

> an intrusion detection system **onboard** the mobile platform and connected to the onboard network for detecting if a potential intrusion event has occurred; and . . .
>
> an onboard security management system responsive to the intrusion detection system for initiating an action to address the potential intrusion event, based on a set of security policies,
>
> wherein:
>
> the action can be directed to at least a selected one of a plurality of user access points on the onboard network;
>
> if an update to the set of policies is necessary, the **policies are updated during the time that the intermittent link has connection** with the terrestrial-based system; and
>
> the onboard security manager maintains an indicator of a current operational state of each one of the plurality of network user access points of the onboard network, wherein the indicator indicates whether at least one of the following conditions is present:
>
> a normal state of operational for the onboard network;
>
> a suspect operational state wherein an intrusion event is suspected; and
>
> a disconnect state in which access by a user of a specific one of the user access points is being prevented (emphasis added).

Claim 34 recites:

> an intrusion detection system **onboard** the mobile platform for monitoring the onboard network for detecting if a potential intrusion event has occurred; and
>
> an **onboard security management system responsive to the intrusion detection system** for initiating an action to address the potential intrusion event, based on a set of security policies, the action able to be directed to at least a selected one of a plurality of user access points on the onboard network;
>
> wherein the action includes one of:
>
> notifying a particular user on the onboard network that a suspected intrusion event has occurred; or
>
> blocking access by the particular user to the onboard network (emphasis added).

Claim 38 recites:

> **using a security management system onboard the mobile platform**, and responsive to notification of an intrusion event, to initiate a security action to address the intrusion event, in accordance with a set of security policies (emphasis added).

Based on the above introduction, Appellant respectfully asserts that neither Huff nor Monroe, singly or in combination, teach, suggest or disclose at least these features.

A. CLAIMS 20-28, 30-31 AND 34-39 ARE NOT OBVIOUS IN VIEW OF HUFF AND MONROE.

In Huff, there is no discussion whatsoever of onboard network accessible to a plurality of users, let alone an intrusion detection system onboard a mobile platform connected to the onboard network and the other recitations of the

system recited in Claims 20, 28, 34 and 38. Further, as noted by the Examiner, Huff does not disclose whatsoever a security system which communicates with a terrestrial-based system. Huff only deals with a system for monitoring either authorized or unauthorized users by two security servers 500, 600 that are located on trucks 700, 732. Furthermore, Huff teaches away from having an onboard network on the same mobile platform as the security system. Huff teaches the desirability of separate vehicles so that the destruction of one vehicle will not alter the security systems 500, 600 or the other computers on each of the vehicles that form the peer-to-peer links. Thus, Huff does not teach, suggest or disclose an intrusion detection system that is onboard the mobile platform for monitoring the onboard network, rather Huff teaches away from an onboard network which is on the same mobile platform as the security system.

Monroe does not remedy the shortcomings of Huff, as Monroe does not disclose or suggest whatsoever an onboard network accessible to a plurality of users or an intrusion detection system onboard the same mobile platform and connected to the onboard network. The primary purpose of Monroe is monitoring the mobile platform "while in port or terminal and/or unattended whether taxing or parked or docked [and] permits tracking while in port or in route [to the port]" through a ground-based communications link (see at least Column 2, Lines 30-51). Monroe further discloses notifying "selected personnel" of a security situation on the mobile platform (see at least Column 7, Lines 59-60). Thus, Monroe provides for monitoring of the mobile platform itself while the mobile platform is in port or on the ground and does not disclose or suggest whatsoever

an intrusion detection system onboard the mobile platform for monitoring an onboard network on the same mobile platform as claimed.

Accordingly, in view of the above discussion, Appellant respectfully asserts the Examiner has not presented a *prima facie* case of obviousness as the cited references fail to teach, suggest or disclose each and every feature of Claims 20, 28, 34 and 38. Thus, Appellant respectfully requests the reconsideration and withdrawal of the rejection of Claims 20, 28, 34 and 38 under 35 U.S.C. § 103(a).

With regard to Claims 21-27, 30, 31, 35-37 and 39, Appellant notes these claims depend directly or indirectly from either independent Claim 20, 28, 34 or 38, and, thus, should be in condition for allowance for the reasons set forth for Claims 20, 28, 34 and 38 above. Accordingly, Appellant respectfully requests the reconsideration and withdrawal of the rejections of Claims 21-27, 30, 31, 35-37 and 39 under 35 U.S.C. § 103(a).

B. THERE IS NO MOTIVATION TO COMBINE HUFF WITH MONROE TO ARRIVE AT CLAIMS 20-28, 30-31 AND 34-39.

First, there is no suggestion in Huff whatsoever regarding the desirability of modifying the security system of Huff for use with the terrestrial based system of Monroe. Appellant submits it is improper for the Office to combine Huff with Monroe to without any express suggestion of the desirability to do so. In particular:

> Obviousness cannot be established by combining the teachings of the prior art to produce the claimed

> invention, absent some teaching or suggestion supporting the combination. Under section 103, **teachings of references can be combined *only* if there is some suggestion or incentive to do so**.

ACS Hosp. Sys., Inc. v. Montefiore Hosp., 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984) (emphasis added). Accordingly, as Huff does not teach or suggest whatsoever a security system for a mobile platform that communicates over a terrestrial-based system, Appellant respectfully asserts the combination of Monroe with Huff is improper.

Second, Appellant respectfully submits it is improper to modify Huff to arrive at Appellant's claims as Huff teaches away from this modification. Specifically:

> It is established that where references, instead of suggesting the invention, **seek or warn to avoid the suggestion**, such references diverge from and teach away from the invention at hand and it is error to find obviousness based on such references.

In re Fine, 837 F.2d 1071, 1074, 5USPQ2d 1596, 1599 (Fed. Cir. 1988) (emphasis added). In this regard, Huff teaches that it is desirable to have separate security systems disposed on separate vehicles so that the destruction of one vehicle will not alter the security systems 500, 600 or the other computers on each of the vehicles that form the peer-to-peer links. Thus, Huff warns against providing the security system onboard the same mobile platform as the network, and thus, Huff teaches away from an intrusion detection system onboard the same mobile platform as the users accessing the mobile network. As Huff expressly teaches the desirability of a security system disposed externally to the onboard network, Appellant submits that one skilled in the art

would not be motivated to modify the Huff reference to arrive at Appellant's claims.

Third, Appellant notes that modifying Huff to include the intrusion diction system onboard the same mobile platform as the onboard network and the users would impermissibly modify the intended purpose and principle of operation of Huff. Specifically, if proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. ***In re Gordon***, 733 F.2d 900,221 USPQ 1125 (Fed. Cir. 1984) MPEP 2143.01.

As modifying Huff to include the security system onboard the same mobile platform as the onboard network and the users would render the system of Huff unsatisfactory for its intended purpose by not providing separate security systems disposed on separate vehicles in case one of the vehicles is destroyed. Thus, Appellant submits that one skilled in the art would not be motivated to modify the Huff reference to arrive at Appellant's claims.

Fourth, it is improper to modify Huff with the teachings of Monroe to arrive at Appellant's claimed subject matter as Huff teaches away from this combination. Specifically, Huff teaches that prior art systems which require human intervention are undesirable as "prior art systems can be circumvented before the human administrator takes action" (see at least Column 11, lines 1-5), while the system of Monroe expressly requires human intervention to respond to the security situation on the mobile platform. Thus, as Huff teaches away from a system including a human administrator, one of ordinary skill in the art would not

be motivated combine the teachings of Monroe with Huff to arrive at Appellant's claims herein.

Fifth, Appellant submits that it is improper to assert that one of ordinary skill, based on the Huff reference, would find it obvious to modify Huff with Monroe to arrive at Appellant's claims herein. In particular, Appellant notes that although one skilled in the art might find it obvious to try various combinations of prior art components, **this is not the standard of 35 U.S.C. § 103**. (In re Geiger, 815 F.2d 686, 688, 2 USPQ2d 1276, 1278 (Fed. Cir. 1987). Rather, in order to find Appellant's claims obvious, the Office must produce both the suggestion and expectation of success in making such a combination. As Huff does not teach, suggest or disclose any desirability in using his security system onboard the same mobile platform as the network and the users, and further, as Huff teaches away from the placement of the security system on the mobile platform, Appellant respectfully asserts the modification of Huff to arrive at Appellant's claims is improper. Further, Appellants note that Huff also does not teach, suggest or disclose whatsoever any desirability in using his security system with a terrestrial-based system over an intermittent link, the combination of Huff with Monroe is improper.

Accordingly, in view of the above discussion, Appellant respectfully asserts that the Examiner has not presented a *prima facie* case of obviousness there is no motivation to modify Huff or to combine Huff with Monroe to arrive at Claims 20, 28, 34 and 38. Thus, Appellant respectfully requests the

reconsideration and withdrawal of the rejection of Claims 20, 28, 34 and 38 under 35 U.S.C. § 103(a).

With regard to Claims 21-27, 30, 31, 35-37 and 39, Appellant notes these claims depend directly or indirectly from either independent Claim 20, 28, 34 or 38, and, thus, should be in condition for allowance for the reasons set forth for Claims 20, 28, 34 and 38 above. Accordingly, Appellant respectfully requests the reconsideration and withdrawal of the rejections of Claims 21-27, 30, 31, 35-37 and 39 under 35 U.S.C. § 103(a).

CONCLUSION

Appellant therefore respectfully submits that neither Huff nor Monroe, teach, suggest or disclose Appellant's Claims 20-28, 30-31 and 34-39 either independently or in any combination. In particular, none of the references cited by the Examiner teach or suggest an onboard network accessible to a plurality of users or an intrusion detection system onboard a mobile platform connected to the onboard network, as recited in Claims 20, 28, 34 and 38. In addition, it is improper to combine Huff with Monroe to arrive at Appellant's claimed subject matter, as Huff teaches away from this modification.

In view of the foregoing, withdrawal of the outstanding rejections of the claims is respectfully requested.

Respectfully submitted,

Dated: 5/2/07

By: _____
Mark D. Elchuk, Reg. No. 33,686
Erica K. Schaefer, Reg. No. 55,861

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1600
MDE/EKS/chs

TABLE OF CONTENTS

EXHIBIT A

CLAIMS APPENDIX

20. In a mobile platform, a security system for monitoring an onboard communication system communicating with a terrestrial-based system over an intermittent link, the security system comprising:

an onboard network accessible to a plurality of users;

an intrusion detection system onboard the mobile platform and connected to the onboard network; and

an onboard security management system responsive to the intrusion detection system for initiating an action to stop intrusion based on a set of policies;

wherein, if an update is necessary, the policies being updated during the time that the intermittent link has connection.

21. The security system as recited in claim 20, wherein initiating the action to stop intrusion comprises sending a warning message to the user.

22. The security system as recited in claim 20, wherein initiating the action to stop intrusion comprises disconnecting the user's access to the onboard network.

23. The security system as recited in claim 20, wherein the onboard security management system further operates to provide an alert message to the terrestrial-based system when an intrusion event is detected.

24. The security system as recited in claim 20, wherein the onboard security management system further operates to install a network traffic blocking filter on one of a plurality of user access points of the onboard network.

25. The security system as recited in claim 20, wherein the action to stop intrusion is directed to a specific one of a plurality of user access points of the onboard network.

26. The security system recited in claim 20, wherein the onboard security manager maintains an indicator of a current operational state of each one of a plurality of network user access points of the onboard network.

27. The security system recited in claim 26, wherein the indicator indicates one of:

a normal operational state;

a suspect operational state wherein an intrusion event is suspected; and

a disconnect state in which access by a user of a specific access point on the onboard network is prevented.

28. In a mobile platform, a security system for monitoring an onboard communication system communicating with a terrestrial-based system over an intermittent link, the security system comprising:

an onboard network accessible to a plurality of users;

an intrusion detection system onboard the mobile platform and connected to the onboard network for detecting if a potential intrusion event has occurred; and

an onboard security management system responsive to the intrusion detection system for initiating an action to address the potential intrusion event, based on a set of security policies;

wherein:

the action can be directed to at least a selected one of a plurality of user access points on the onboard network;

if an update to the set of policies is necessary, the policies are updated during the time that the intermittent link has connection with the terrestrial-based system; and

the onboard security manager maintains an indicator of a current operational state of each one of the plurality of network user access points of the

onboard network, wherein the indicator indicates whether at least one of the following conditions is present:

a normal state of operational for the onboard network;

a suspect operational state wherein an intrusion event is suspected; and

a disconnect state in which access by a user of a specific one of the user access points is being prevented.

30. The security system as recited in claim 28, wherein the onboard security manager notifies the terrestrial-based system when the potential intrusion event is detected.

31. The security system as recited in claim 28, wherein the action comprises preventing access to the onboard network from a selected one or more of the user access points from the onboard network.

34. In a mobile platform, a security system for monitoring an onboard communication system communicating with a terrestrial-based system over an intermittent link, the security system comprising:

an onboard network accessible to a plurality of users;

an intrusion detection system onboard the mobile platform for monitoring the onboard network for detecting if a potential intrusion event has occurred; and

an onboard security management system responsive to the intrusion detection system for initiating an action to address the potential intrusion event, based on a set of security policies, the action able to be directed to at least a selected one of a plurality of user access points on the onboard network;

wherein the action includes one of:

notifying a particular user on the onboard network that a suspected intrusion event has occurred; or

blocking access by the particular user to the onboard network.

35. The security system recited in claim 34, wherein the onboard security management system receives updates to said security policies from the terrestrial-based system while said intermittent link is operational.

36. The security system recited in claim 34, wherein the onboard security management system notifies the terrestrial-based system that a potential intrusion event has occurred.

37. The security system recited in claim 34, where the action taken by the onboard security management system further includes installing a network traffic blocking filter on said user access point on which a potential intrusion event has occurred.

38. A method for monitoring an onboard network on a mobile platform, in which the onboard network is in intermittent communication with a terrestrial-based system, the method comprising:

providing a plurality of network access points to users on the mobile platform;

monitoring the onboard network to detect for an intrusion event; and

using a security management system onboard the mobile platform, and responsive to notification of an intrusion event, to initiate a security action to address the intrusion event, in accordance with a set of security policies.

39. The method recited in claim 38, further comprising updating the security policies while the onboard network is in communication with the terrestrial-based system.

EXHIBIT B

EVIDENCE APPENDIX

None.

EXHIBIT C

RELATED PROCEEDINGS APPENDIX

None.